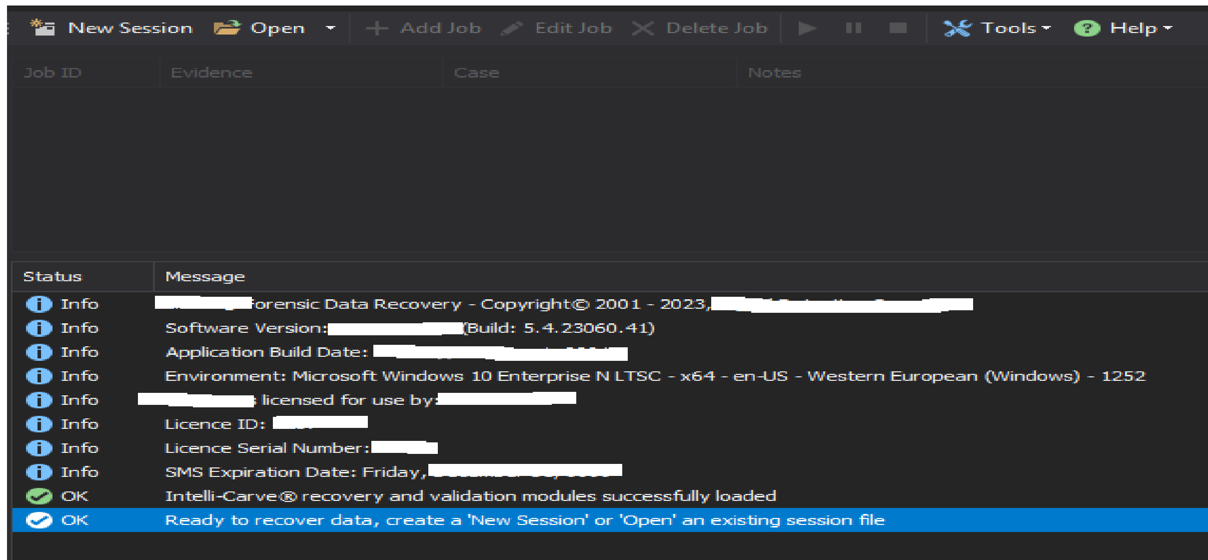
BROWSER FORENSICS WITH COMMERCIAL TOOLS

Aung Zaw Myo

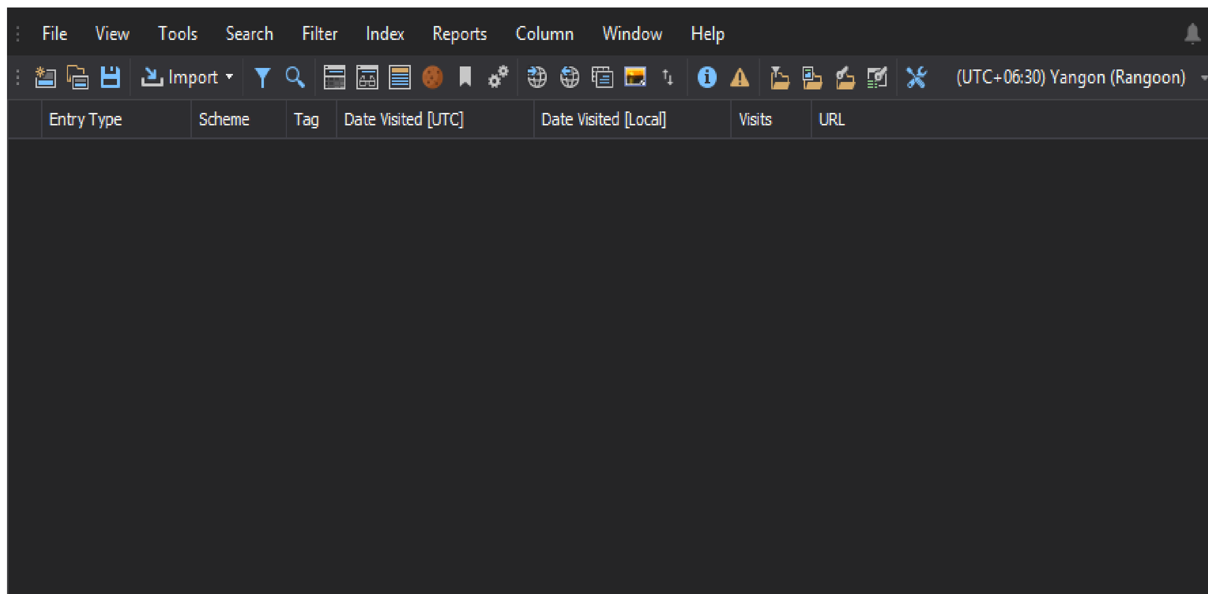
www.forensicsmyanmar.com

BROWSER FORENSICS WITH COMMERCIAL TOOLS

အခုဖော်ပြမဲ့ Browser History Recovery , Analysis Application ကို Law Enforcement Agency, Organization, IT Company တွေအများဆုံးအသုံးပြုလျှက်ရှိပါတယ်။ သူ့မှာ Browser History ကို Recovery ပြုလုပ်တဲ့အပိုင်းနဲ့ ရလာတဲ့ Browser History ကို Analysis ပြုလုပ်တဲ့ အပိုင်းဆိုပြီး နှစ်ခုရှိပါတယ်။

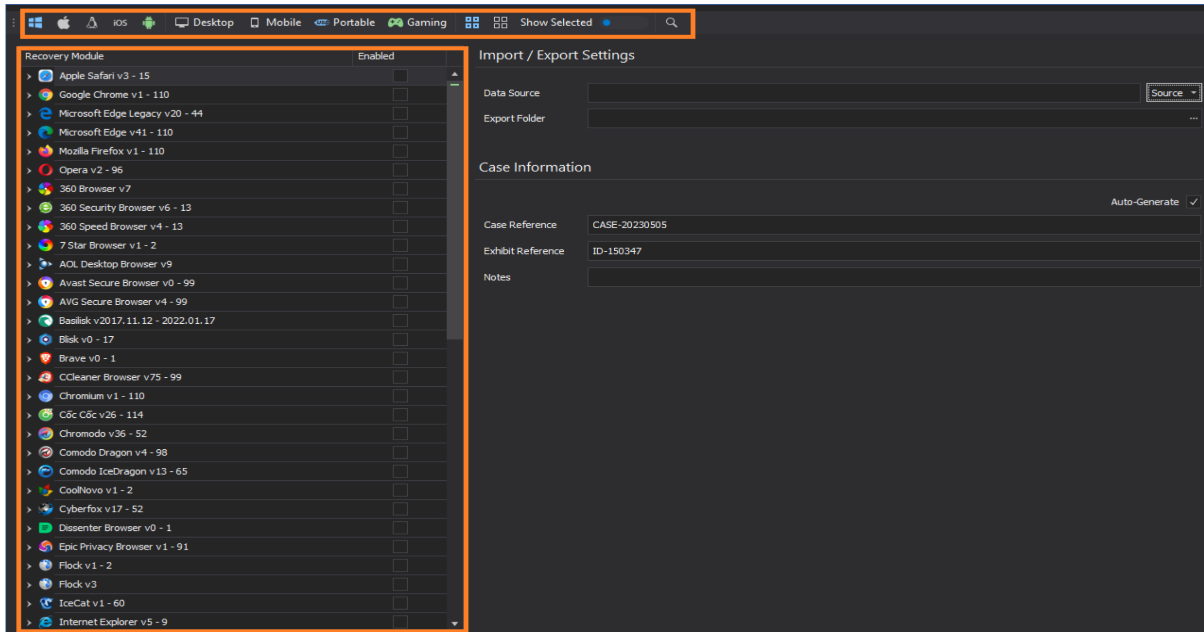


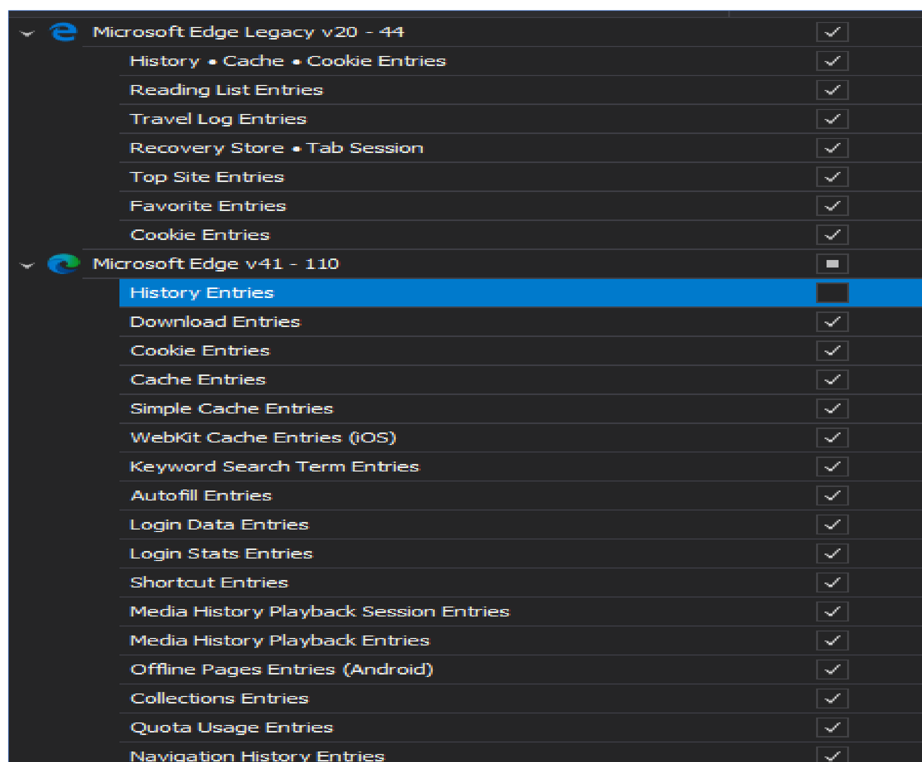
Recovery Computer and Mobile Browser History

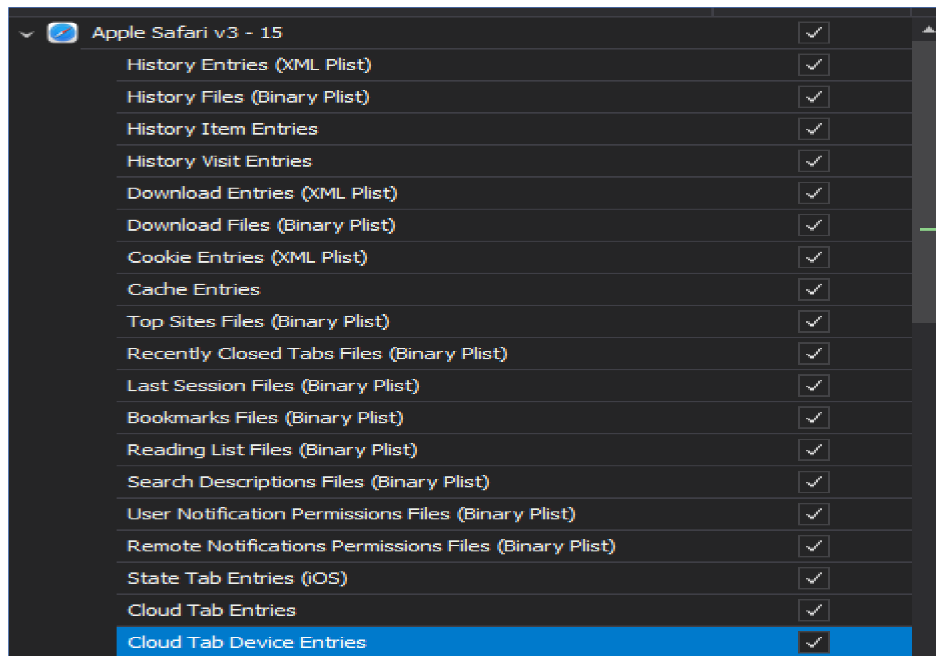


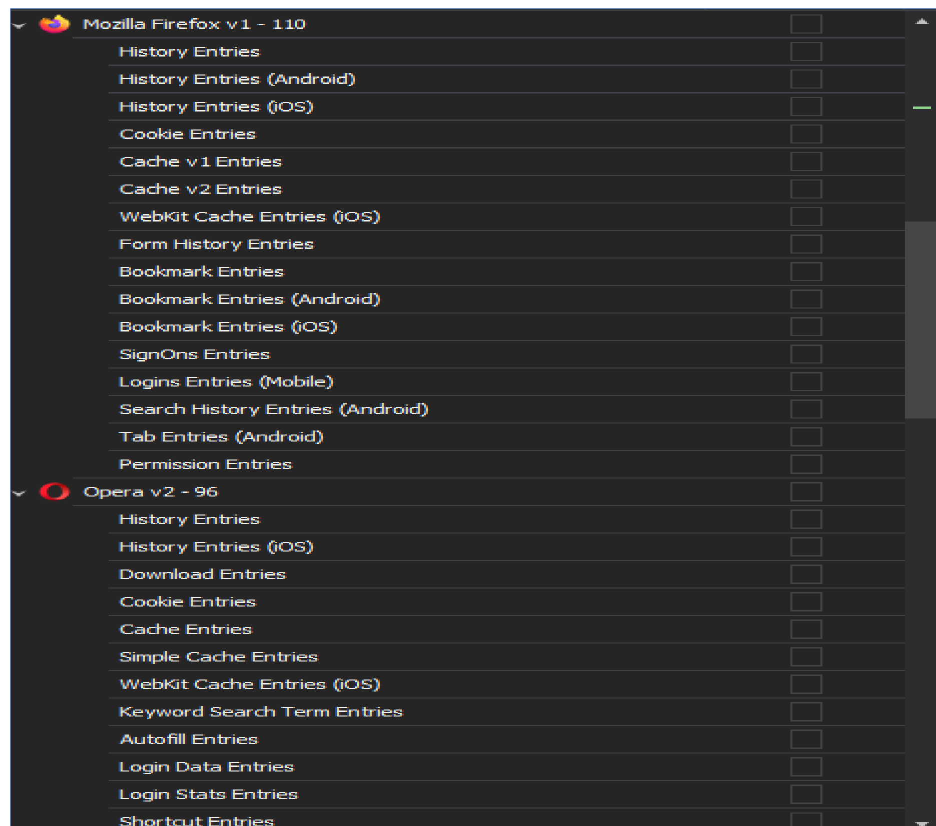
Analysis Recovered Browser History

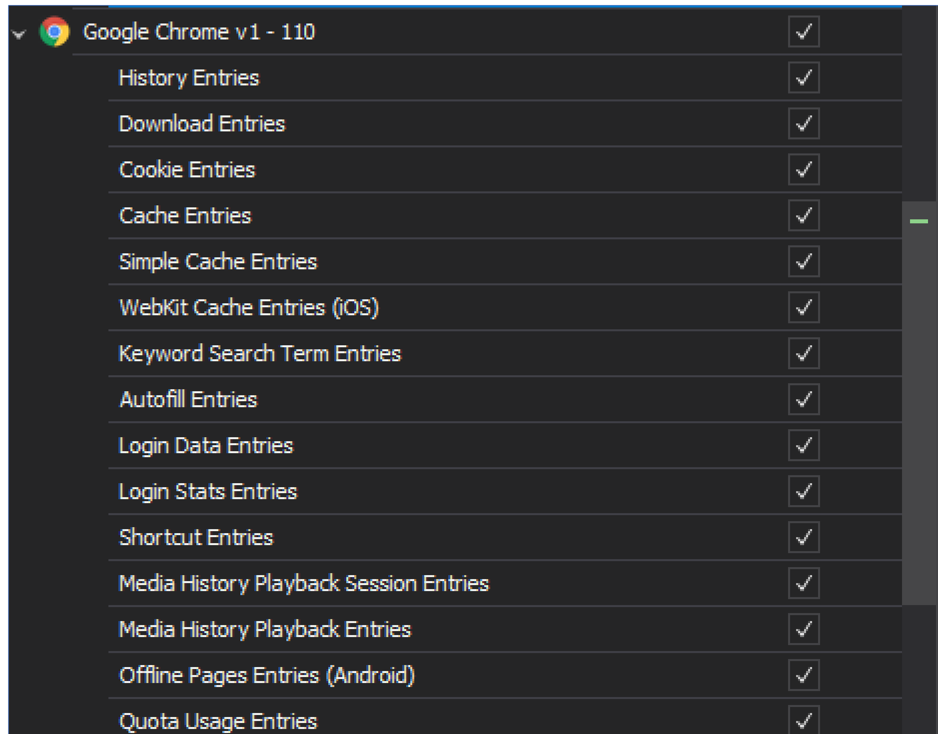
အောက်မှာဖော်ထားတာကတော့ Recovery and Analysis ပြုလုပ်နိုင်တဲ့ Browser Artifacts တွေဖြစ်ပါတယ်။ Support လုပ်တာကတော့ Desktop, Mobile မှာအသုံးပြုတဲ့ Browser 90 ကျော်ကို Support ပြုလုပ်ပါတယ်။ အခု PDF မှာတော့ Major Computer Browser တွေကို ဖော်ပြထားပါတယ်။



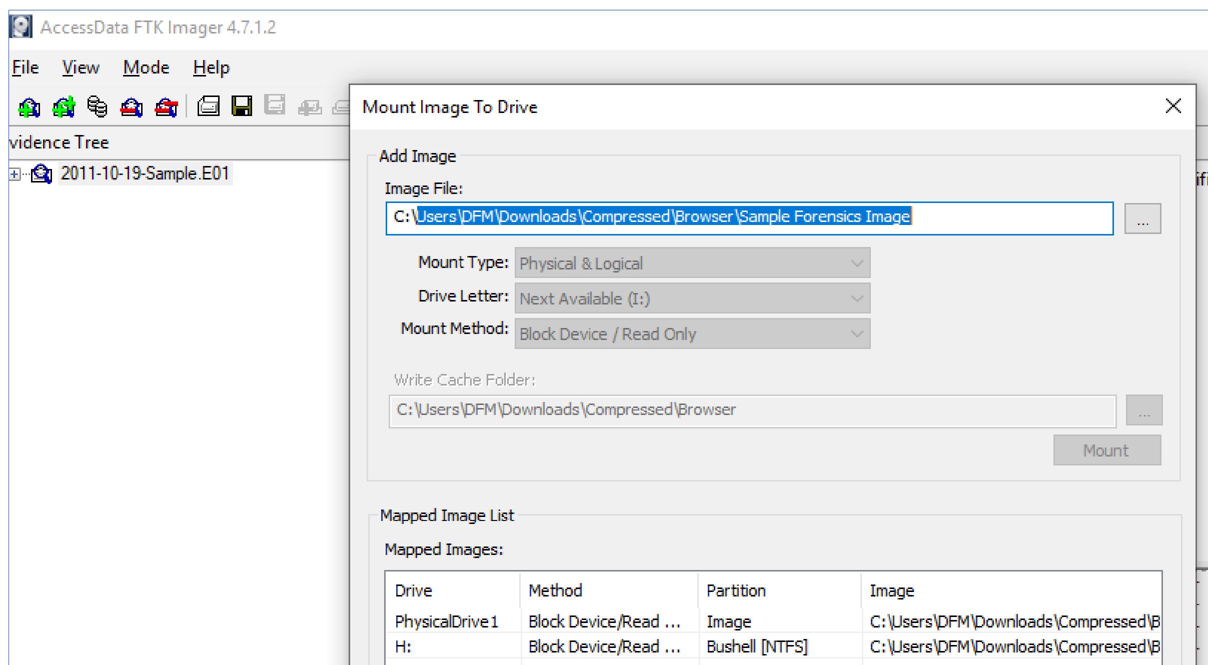



Apple Safari v3 - 15
History Entries (XML Plist)
History Files (Binary Plist)
History Item Entries
History Visit Entries
Download Entries (XML Plist)
Download Files (Binary Plist)
Cookie Entries (XML Plist)
Cache Entries
Top Sites Files (Binary Plist)
Recently Closed Tabs Files (Binary Plist)
Last Session Files (Binary Plist)
Bookmarks Files (Binary Plist)
Reading List Files (Binary Plist)
Search Descriptions Files (Binary Plist)
User Notification Permissions Files (Binary Plist)
Remote Notifications Permissions Files (Binary Plist)
State Tab Entries (iOS)
Cloud Tab Entries
Cloud Tab Device Entries


Mozilla Firefox v1 - 110
History Entries
History Entries (Android)
History Entries (iOS)
Cookie Entries
Cache v1 Entries
Cache v2 Entries
WebKit Cache Entries (iOS)
Form History Entries
Bookmark Entries
Bookmark Entries (Android)
Bookmark Entries (iOS)
SignOns Entries
Logins Entries (Mobile)
Search History Entries (Android)
Tab Entries (Android)
Permission Entries
Opera v2 - 96
History Entries
History Entries (iOS)
Download Entries
Cookie Entries
Cache Entries
Simple Cache Entries
WebKit Cache Entries (iOS)
Keyword Search Term Entries
Autofill Entries
Login Data Entries
Login Stats Entries
Shortcut Entries

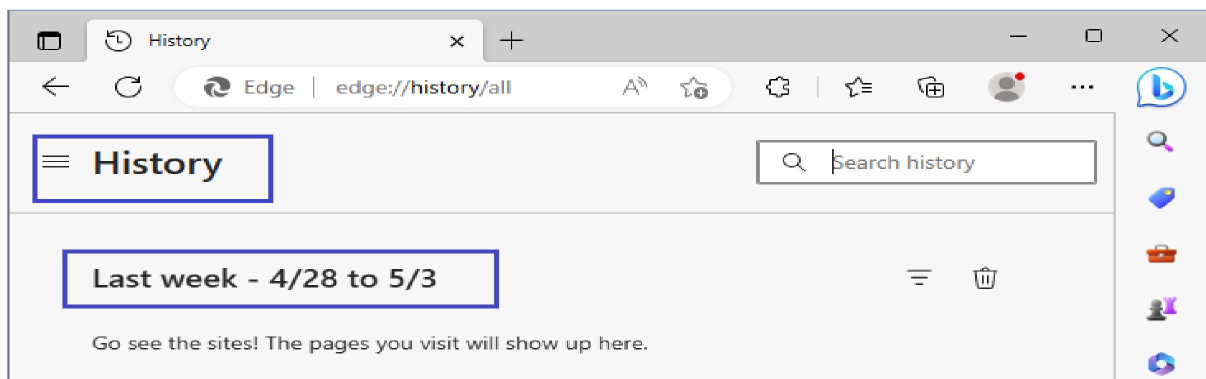


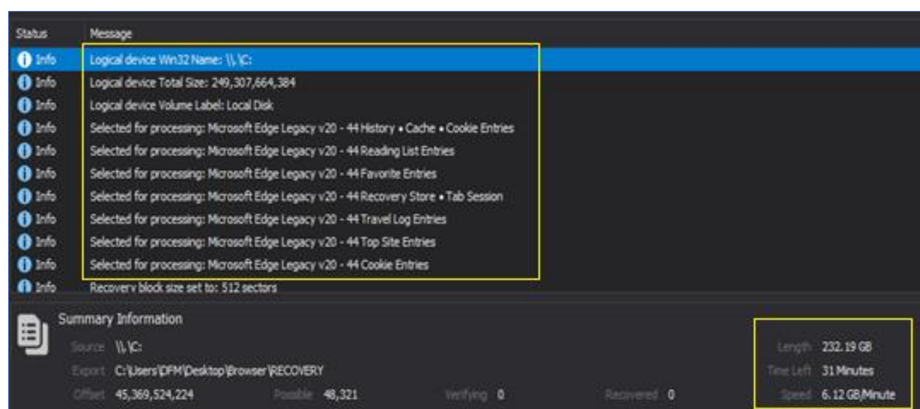
Recovery ပြုလုပ်ရာမှာ Physical Disk, Logical Disk, Forensics Image တွေကနေ Recovery ပြုလုပ်နိုင်ပါတယ်။ Forensics Image ကို FTK Imager မှာ Mount ပြုလုပ်ပြီးတော့လဲ Recovery and Analysis အပိုင်းကိုပြုလုပ်နိုင်ပါတယ်။

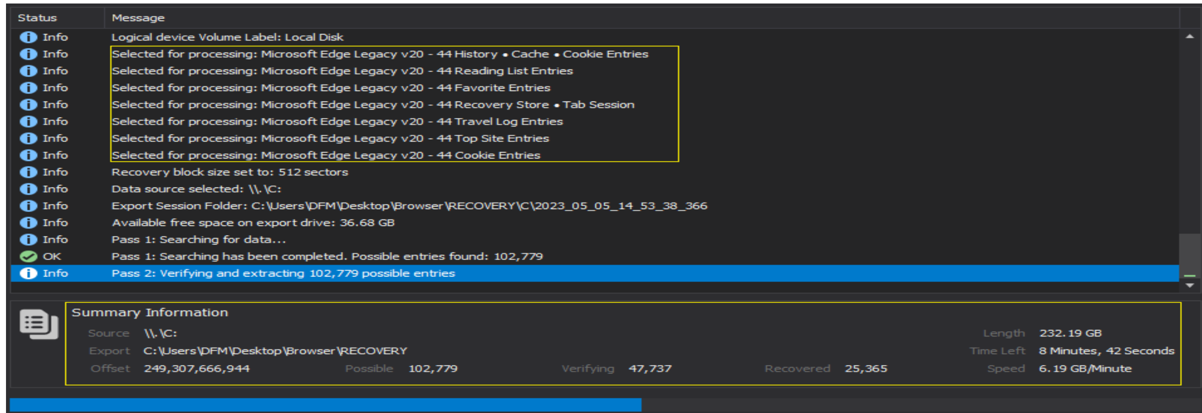


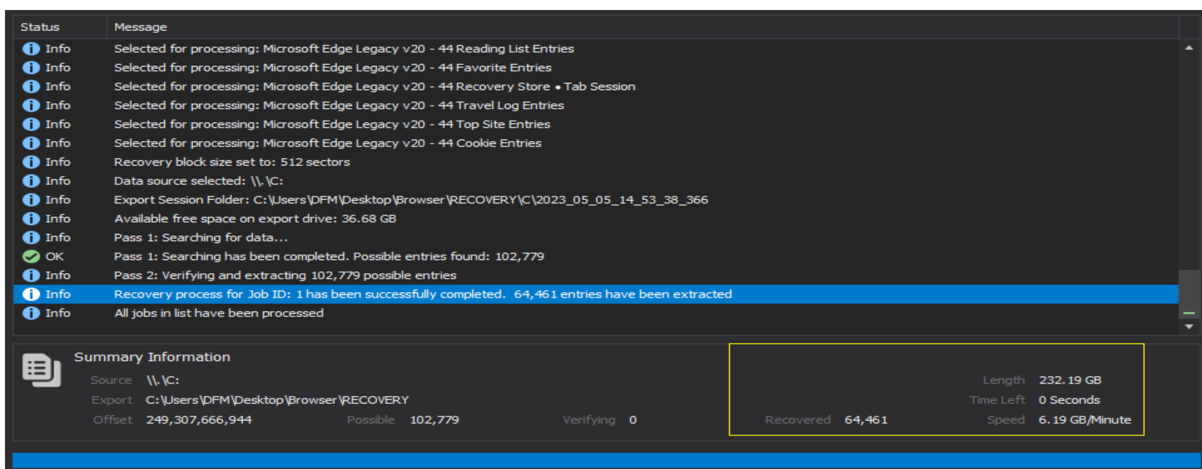
EnCase® v1-7 Image (*.e01)
Memory Dump (*.dmp; *.dump; *.crash; *.mem; *.vmem; *.mdmp)
AccessData® Image (*.e01;*.001,*.s01)
Smart Image (*.s01)
Micro Systemation Extraction File (*.xry)
VMWare Virtual Disk File (*.vmdk)
Virtual Hard Disk File (*.vhd)
Segmented Raw Image (*.000;*.0000;*.00000;*.001;*.0001;*.00001)
Single Raw Image (*.dd;*.img;*.ima;*.raw)
EnCase® v7+ Image (*.ex01)
Zip Archive (*.zip)
Binary Dump (*.Bin; *.dat; *.unallocated; *.rec; *.data; *.binary)

အပေါ်ကပုံကတော့ Analysis ပြုလုပ်တဲ့ Application မှာ Support ပြုလုပ်တဲ့ Forensics Image and File Extension တွေဖြစ်ပါတယ်။ ဥပမာအနေနဲ့ Local Disk C: ကို Recovery ပြုလုပ်ထားပါတယ်။ Recovery မပြုလုပ်ခင် Edge Browser ရဲ့ History ကို Clear Browser History ပြုလုပ်ထားပါတယ်။ **တစ်ကယ်တန်း Analysis ပြုလုပ်ဖို့အတွက် Browser History က အရေးကြီးတယ်ဆိုရင် Logical Disk တစ်ခုတည်းကိုပဲ Recovery မပြုလုပ်ပဲ Physical Disk တစ်ခုလုံးကို Recovery ပြုလုပ်သင့်ပါတယ်။**

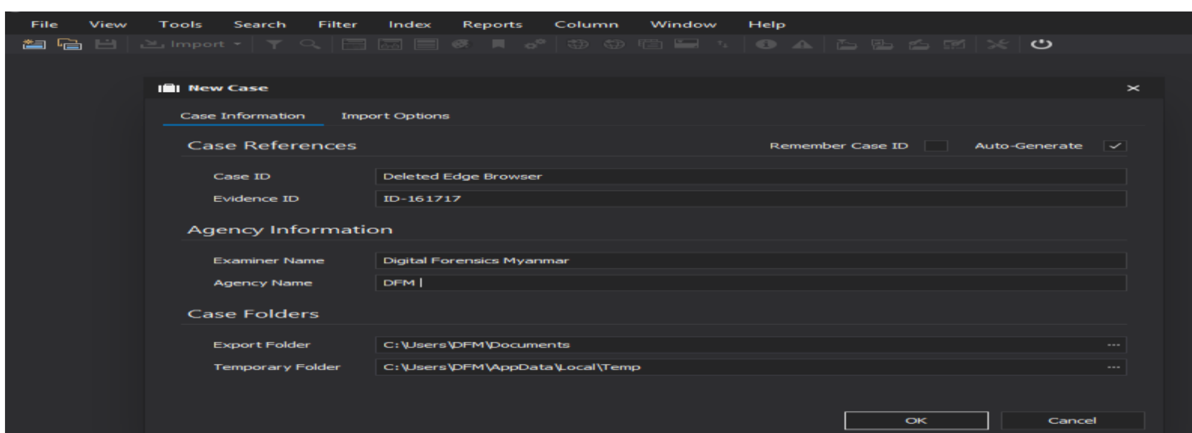


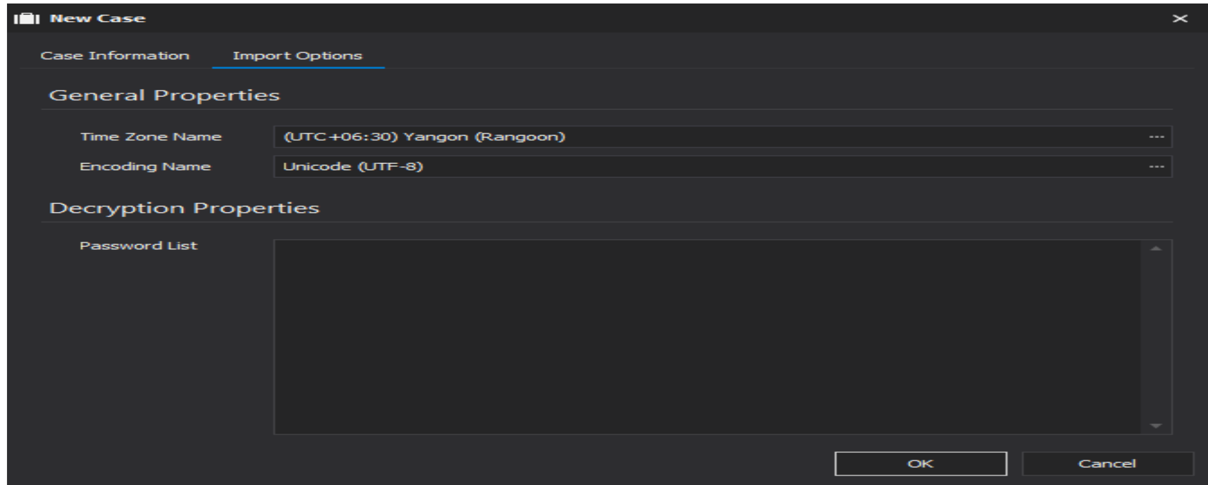


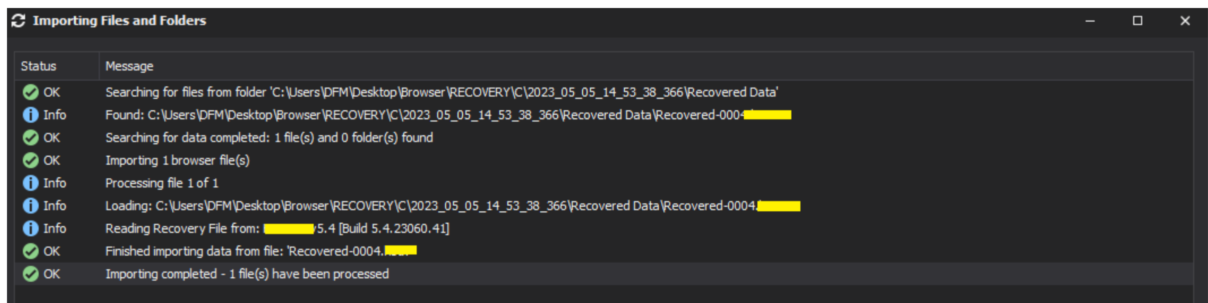


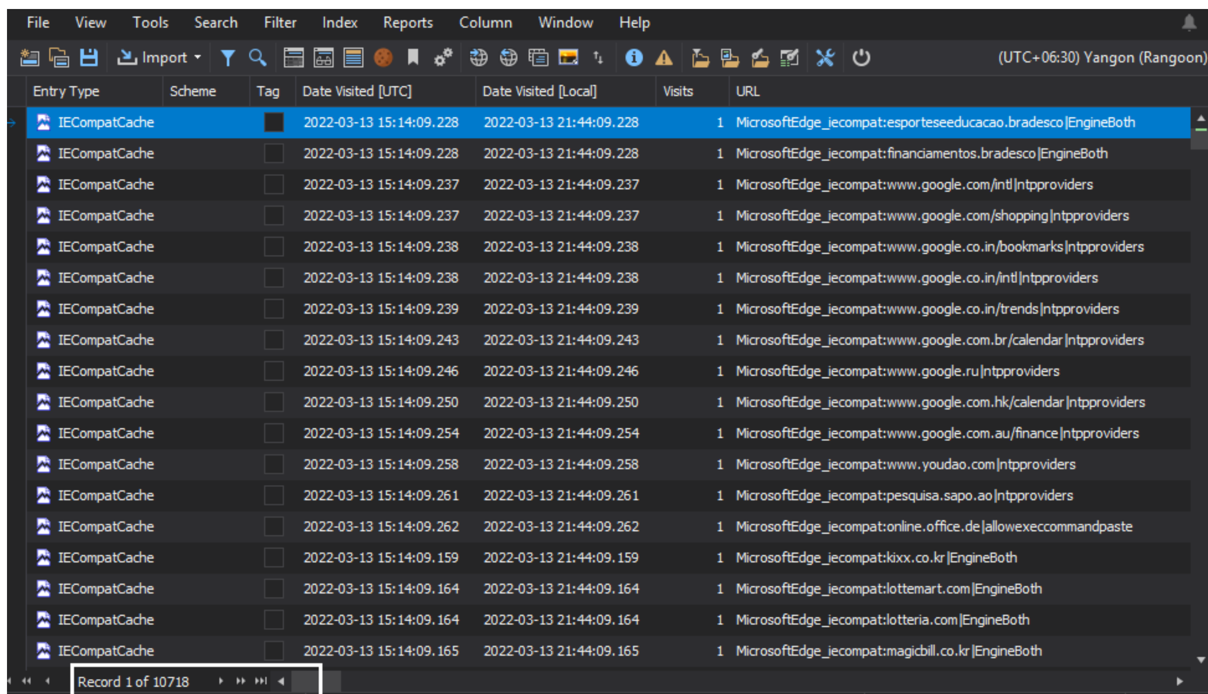


Recovery Process ပြီးတဲ့အခါမှာ Analysis App ထဲကိုထည့်ဖို့အတွက်လိုအပ်တဲ့ Information, Time Zone ကိုရွေးချယ်ရမှာဖြစ်ပါတယ်။ Time Zone ရွေးတဲ့အခါမှာ ကိုယ် Analysis ပြုလုပ်မဲ့ Computer, Mobile မှာရှိတဲ့ Time Zone ကိုရွေးချယ်ရမှာဖြစ်ပါတယ်။



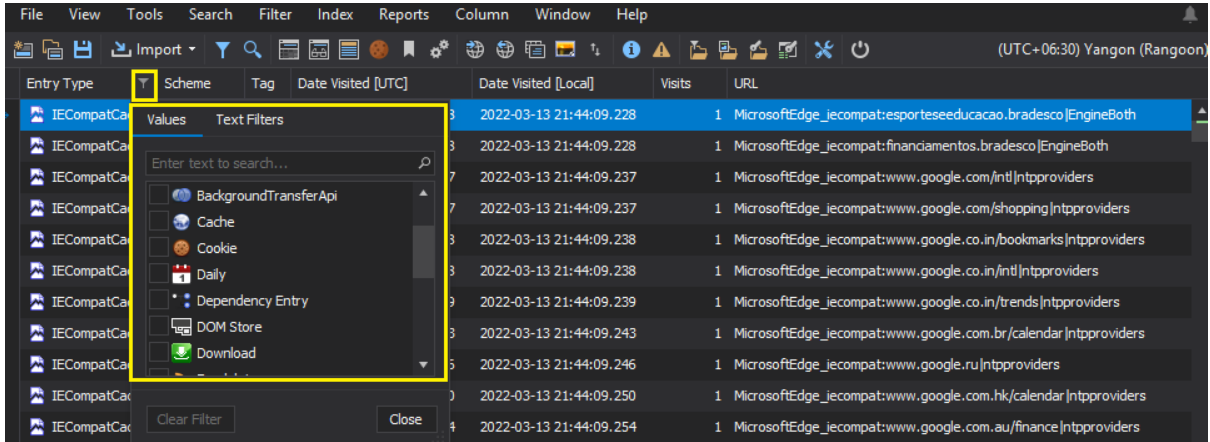




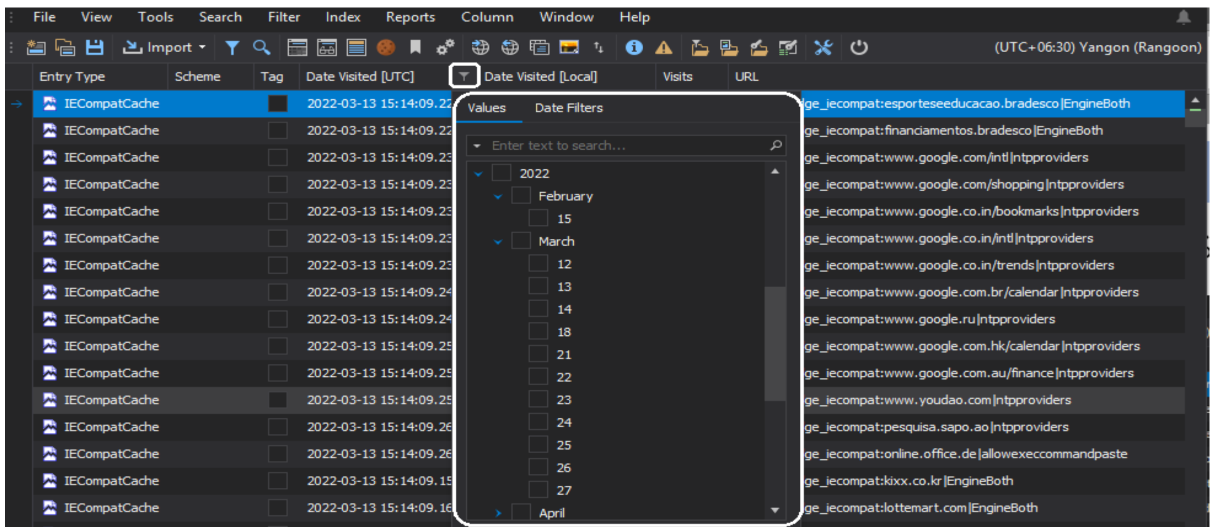


Import ပြုလုပ်ပြီးတဲ့အချိန်မှာ Record 10718 ခုရှိတာကို တွေ့ရမှာဖြစ်ပါတယ်။

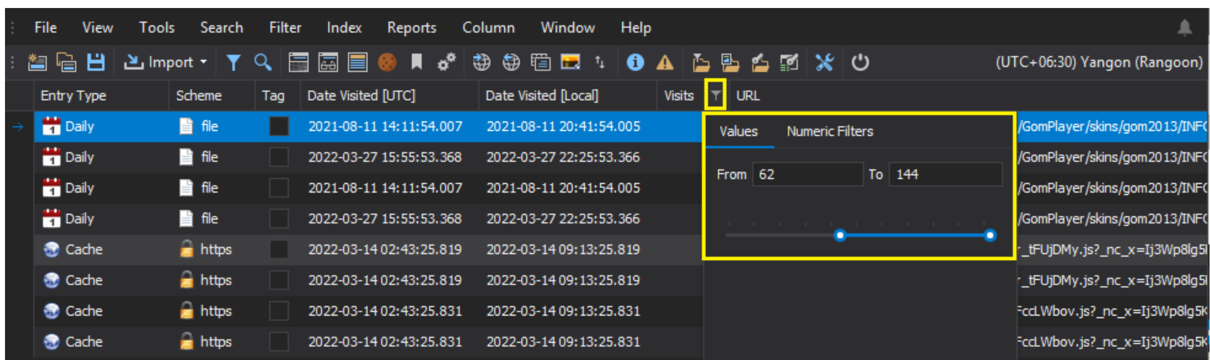
Record တွေက များတဲ့အတွက် ကိုယ်လိုချင်တဲ့အပိုင်းကို Filter တွေနဲ့ စစ်ဆေးနိုင်ပါတယ်။



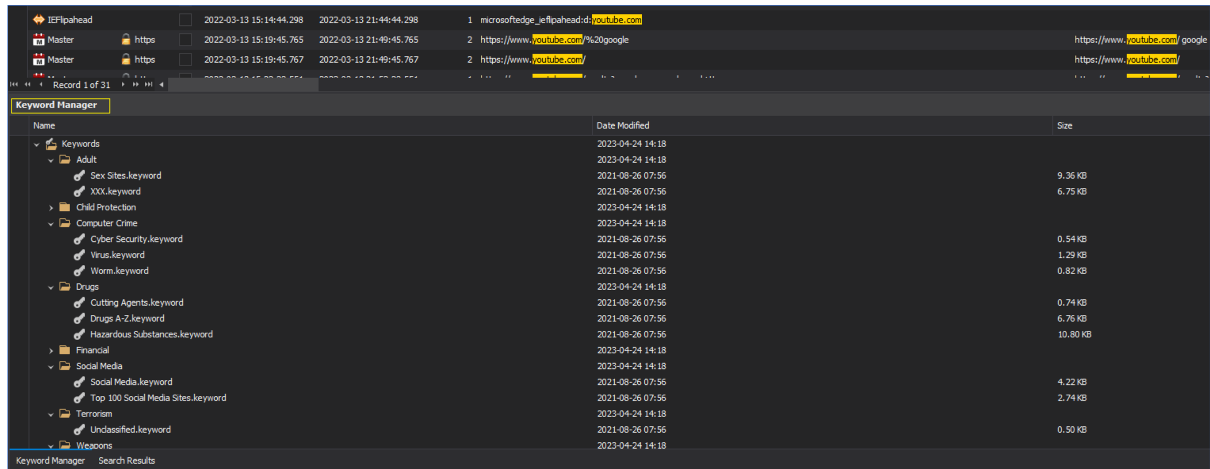
Entry Type Filter



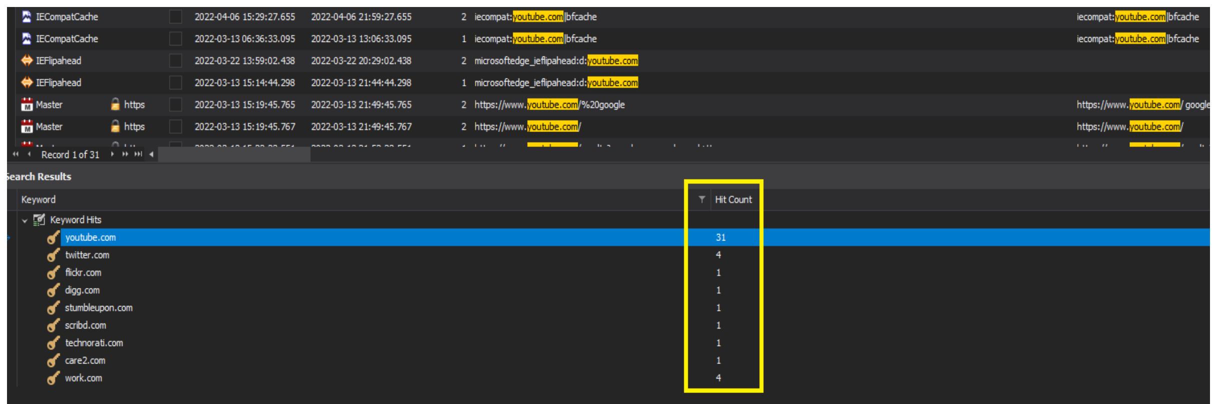
Date Time Filter



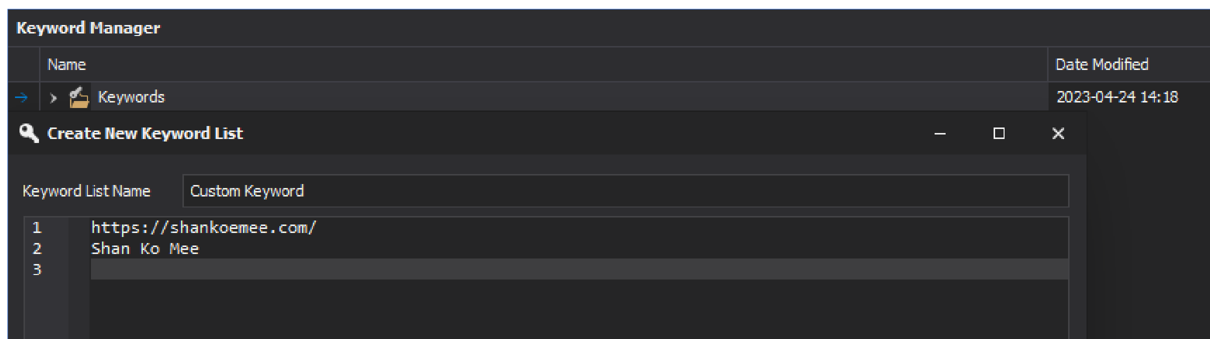
Visited Time Filter



Keyword Search

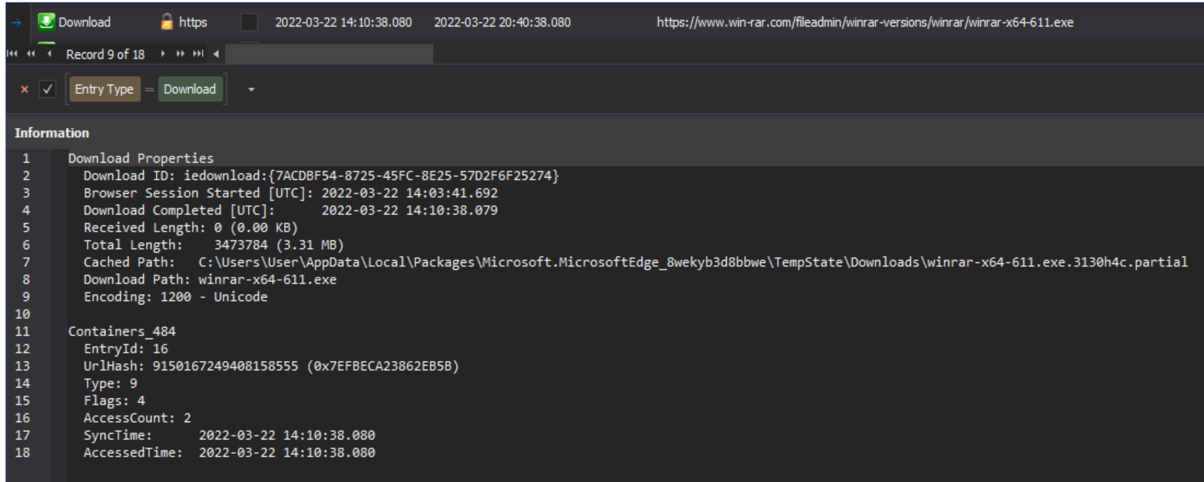


Keyword Search

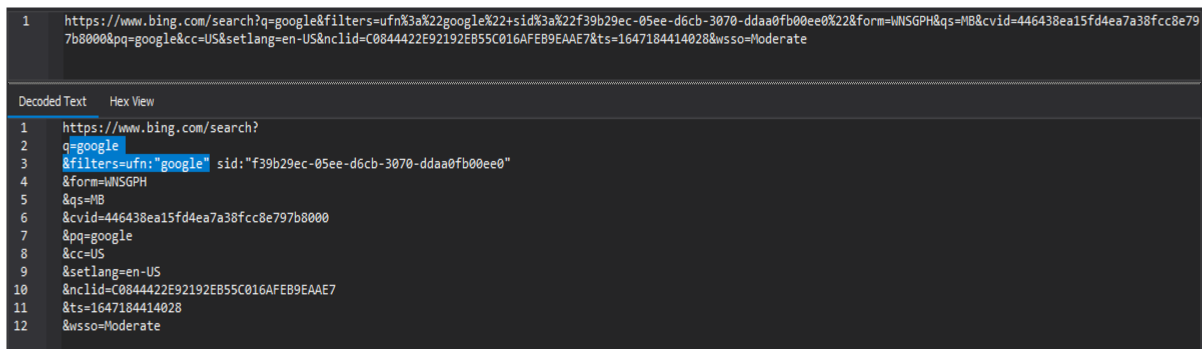


Custom Keyword

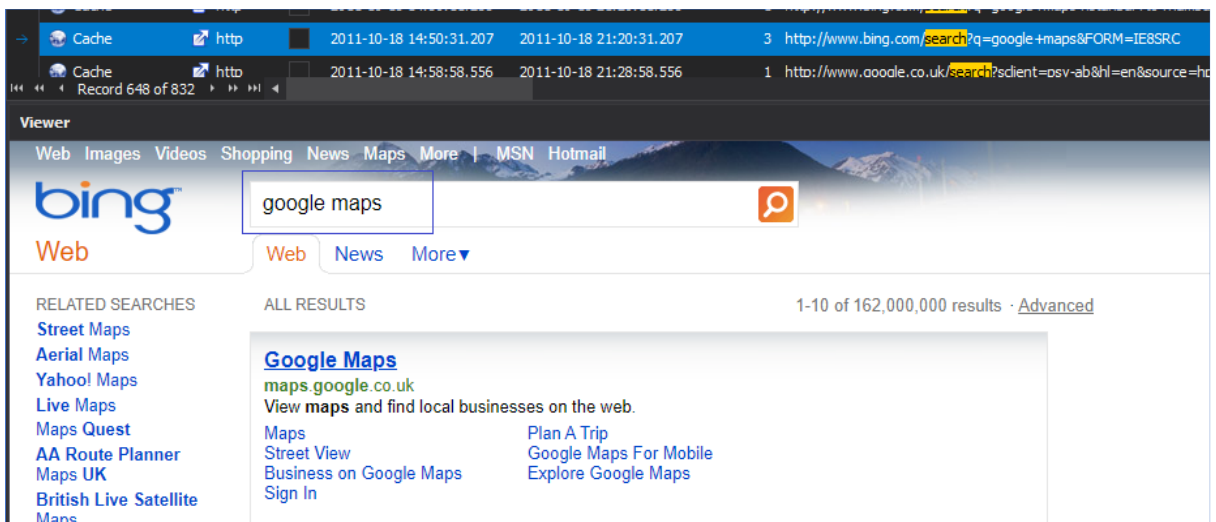
Keyword Search မှာ သက်ဆိုင်ရာအပိုင်းအလိုက် Default ပါတဲ့ Keywords တွေရှိသလို ကိုယ်ရှာဖွေလိုတဲ့ Keywords တွေကို Custom အနေနဲ့သတ်မှတ်လို့ရပါတယ်။



History တစ်ခုရဲ့ Detail Information ဖြစ်ပါတယ်။



URL Decoding



History တစ်ခုကို Offline Web View အနေနဲ့ကြည့်နိုင်ပါတယ်။

Cookie Examiner

Name	Value
UID	
Domain	scorecardresearch.com
Path	/
Date Last Modified [UTC]	2022-03-22 14:11:26.935
Date Expiration [UTC]	2024-03-11 14:11:26.935
HTTP Only	False
Secure	True
Information	Server-Side (Persistent)
Original Value	1703dd81d192bf77f19c7e61647224085

Drag column header here to group by that column

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cookie			2022-03-22 14:11:26.935	2022-03-22 20:41:26.935		scorecardresearch.com
Cookie			2022-03-22 14:11:26.935	2022-03-22 20:41:26.935		scorecardresearch.com

Cookie Examiner

Cookie Examiner

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
Cache	http		2011-10-18 15:03:39.194	2011-10-18 21:33:39.194	1	http://www.bing.com/search?q=how+to+mask+firearm+smell&FORM=IE8SRC

Search Index

gun

URN	File Path
3141	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003141.txt
3173	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003173.txt
3168	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003168.txt
3139	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003139.txt
3087	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003087.txt
3091	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000003091.txt
623	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000000623.txt
909	C:\Users\DFM\Documents\CASE-20230508\ID-115053\Internet Explorer\HTML to Text\F0000000909.txt

Record 3 of 8

how to mask firearm smell - Bing

Web
Images
Videos
Shopping
News
Maps
More
|
MSN
Hotmail
Sign in
United Kingdom
Preferences
Bing
Web
Web

Record 1 of 1

URN = 3168

Viewer

Web Images Videos Shopping News Maps More | MSN Hotmail

bing Web

how to mask firearm smell

Web More▾

RELATED SEARCHES
How to Smell Sweet
How to Smell Sexy
How to Smell Manly
How to Smell Breath
How to Smell Younger

ALL RESULTS

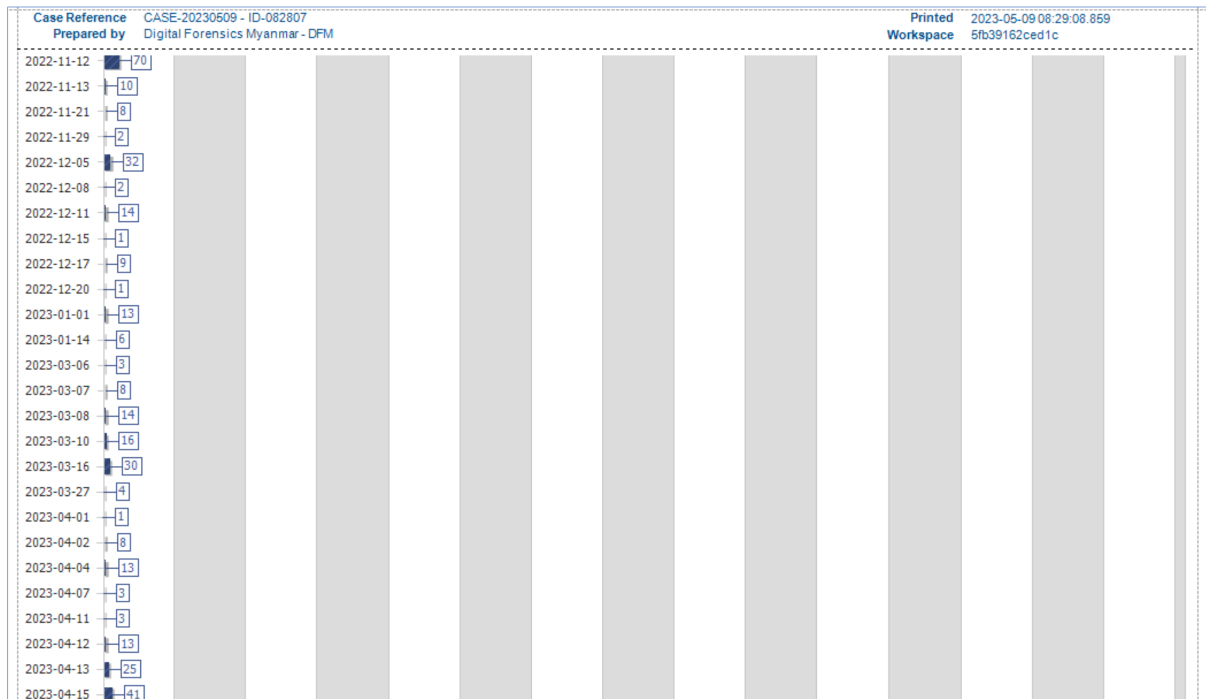
love the smell of powder in the air - Maryland Shooters
7 replies from June 2011
love the smell of powder in the air ... "...beneath this mask there is more th
Utah Concealed Firearm Permit Course Schedule October 9 VFW ...
www.mdshooters.com/showthread.php?t=60361

Indexing, Searching

Forensics Report အနေနဲ့ ကိုယ်လိုချင်တာကို ရွေးချယ်သတ်မှတ်ပြီး Report ထုတ်နိုင်ပါတယ်။ ဥပမာ အနေနဲ့ Search လုပ်ထားတဲ့ Keywords တွေကိုပဲ ရွေးချယ်ပြီး Report ပြုလုပ်ထားပါတယ်။ နောက်တစ်ခုကတော့ Graphic Report အနေနဲ့ နေ့စဉ်သုံးစွဲတာကို Report ပြုလုပ်ထားပါတယ်။

Search Term	Date Visited [Local]	Date Visited [UTC]	Record URN	Page Title	URL
google	2022-03-13 13:26:02.129	2022-03-13 06:56:02.129	9274		https://www.bing.com/search?q=google&src=IE-SearchBox&FORM=IE11SR&pc=EUPP_
winRAR 64 Download	2022-03-13 13:26:34.060	2022-03-13 06:56:34.060	9275		https://www.bing.com/th?q=winRAR+64+Download&w=100&h=100&c=7&rs=1&p=0&o=5&pid=1.7&mkt=en-WW&cc=MM&setlang=en&adlt=moderate&t=1
winRAR Archiver	2022-03-13 13:39:48.792	2022-03-13 07:09:48.792	9281		https://www.bing.com/th?q=winRAR+Archiver&w=100&h=100&c=7&rs=1&p=0&o=5&pid=1.7&mkt=en-WW&cc=MM&setlang=en&adlt=moderate&t=1
winRAR Software	2022-03-13 13:39:48.885	2022-03-13 07:09:48.885	9286		https://www.bing.com/th?q=winRAR+Software&w=100&h=100&c=7&rs=1&p=0&o=5&pid=1.7&mkt=en-WW&cc=MM&setlang=en&adlt=moderate&t=1
winRAR Archiver	2022-03-13 13:39:48.792	2022-03-13 07:09:48.792	9293		https://www.bing.com/th?q=winRAR+Archiver&w=100&h=100&c=7&rs=1&p=0&o=5&pid=1.7&mkt=en-WW&cc=MM&setlang=en&adlt=moderate&t=1
google	2022-03-13 13:34:55.889	2022-03-13 07:04:55.889	9301		https://www.bing.com/news/NewsAnswerV2CarouselAjax?q=google&width=608&IG=4A5EA87C025248658134EB69BB3F9CDA&IID=NEWS.401&SFX=0&disablecarousel=1&OMWQ=0
Google.com Search	2022-03-13 13:34:47.433	2022-03-13 07:04:47.433	9329		https://www.bing.com/th?q=Google.com+Search&w=100&h=100&c=7&rs=1&p=0&o=5&pid=1.7&mkt=en-WW&cc=MM&setlang=en&adlt=moderate&t=1

Browser Search Report

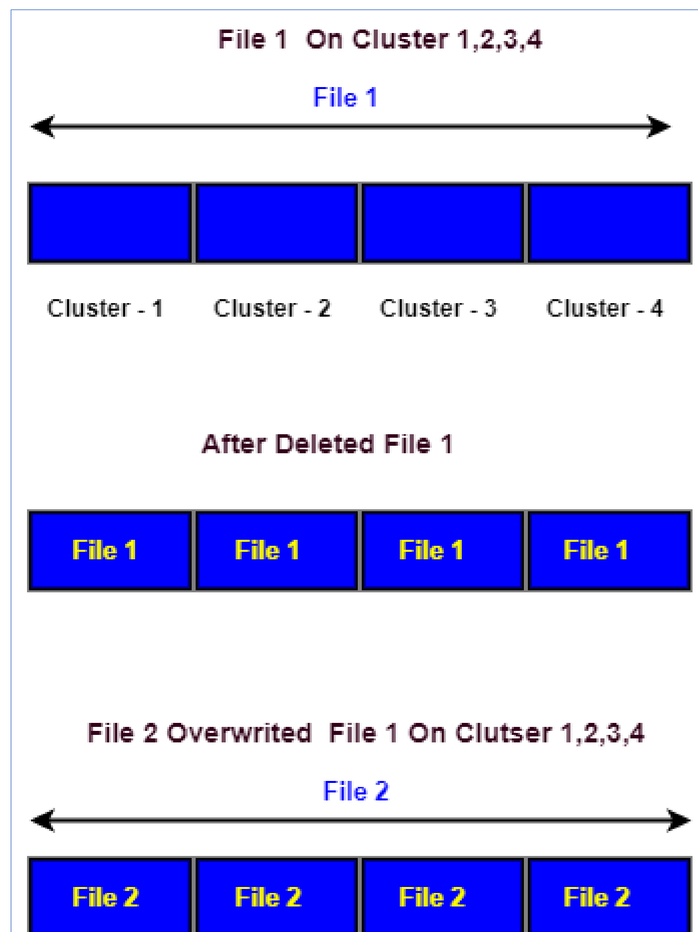


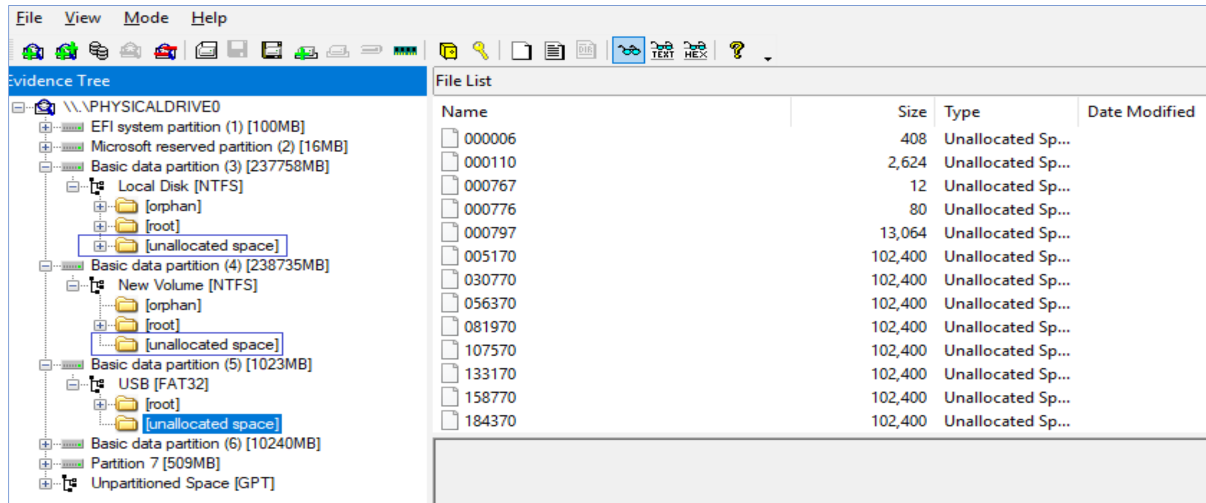
Daily Usage Report

Analysis အပိုင်းကတော့ Application ကိုတစ်ပတ်လောက် အသုံးပြုလိုက်တာနဲ့ အလွယ်တစ်ကူ အသုံးပြုနိုင်မှာ ဖြစ်ပါတယ်။ Edge Browser ကနေ History ရှင်းထားတာကို ဘာလို့ အချို့သော Record တွေက Recovery လုပ်တဲ့အချိန်မှာ ရရှိလာတာလဲဆိုရင်......

Unallocated Cluster, Unallocated Space

ကျွန်တော်တို့ Storage ထဲမှာရှိတဲ့ File တစ်ခုကို Delete လုပ်လိုက်ရင် မျက်စိအမြင် မှာသာ File က ပျောက်သွားပေမဲ့ Storage ရဲ့ Cluster တွေပေါ်မှာရှိနေဆဲဖြစ်ပါတယ်။ ဒါကို Unallocated Cluster, Unallocated Space လို့ခေါ်ပါတယ်။ အဲဒီအချိန်က Recovery ပြုလုပ်လို့ရနိုင်တဲ့ အခြေအနေဖြစ်ပါတယ်။ ဒါပေမဲ့ နောက်ထပ် File တစ်ခုက စောနက File ဖျက်လိုက်တဲ့ Cluster တွေပေါ်မှာ နေရာယူသွားမယ်ဆိုရင် Overwrite ဖြစ်ပြီး Recovery ပြုလုပ်လို့မရနိုင်တော့ပါ။ ပိုပြီးရှင်းအောင် ပုံနဲ့ပြသထား ပါတယ်။ ပုံကို Cluster အနေနဲ့မကြည့်ပဲ Sector အနေနဲ့လဲကြည့်နိုင်ပါတယ်။

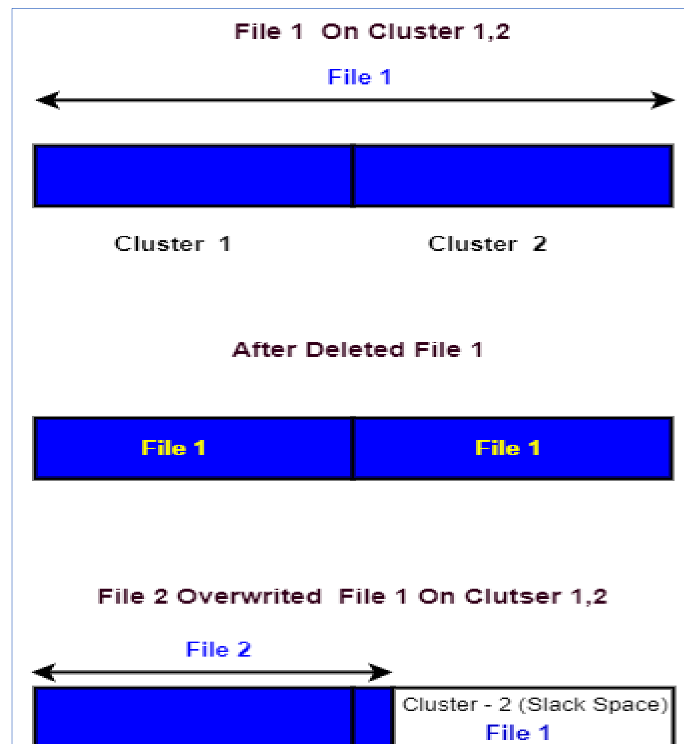




Unallocated Space

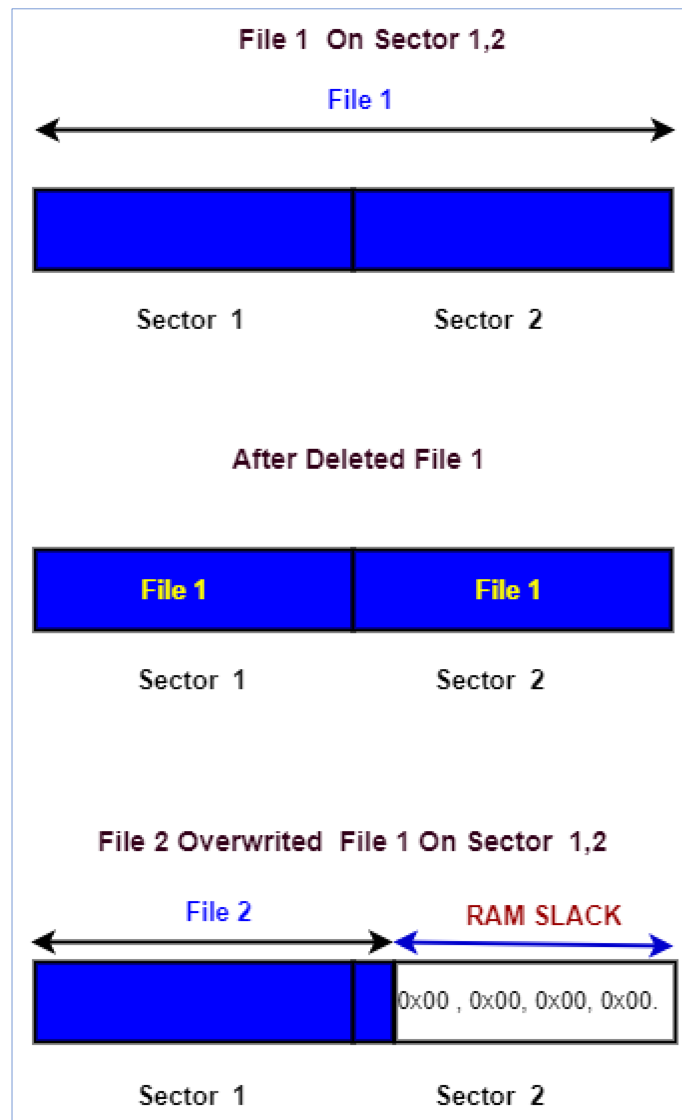
Cluster Slack, Slack Space

ကျွန်တော်တို့ File တစ်ခုကို Storage ပေါ်သိမ်းဆည်းတဲ့အခါမှာ File Size က Cluster Size တွေရဲ့ ပမာဏထက်ငယ်နေရင် Cluster Slack, Slack Space တွေဖြစ်ပေါ်လာ ပါတယ်။ Slack Space တွေက Sector, Cluster Size အနေနဲ့ကြည့်ရင် မသိသာပေမဲ့ Storage တစ်ခုလုံးအနေနဲ့ဆိုရင် Forensics Evidences တွေရှိနိုင်ပါတယ်။ Sector တွေပေါင်းထားတဲ့ အစုအဝေးကို Cluster လို့သတ်မှတ်ပါတယ်။



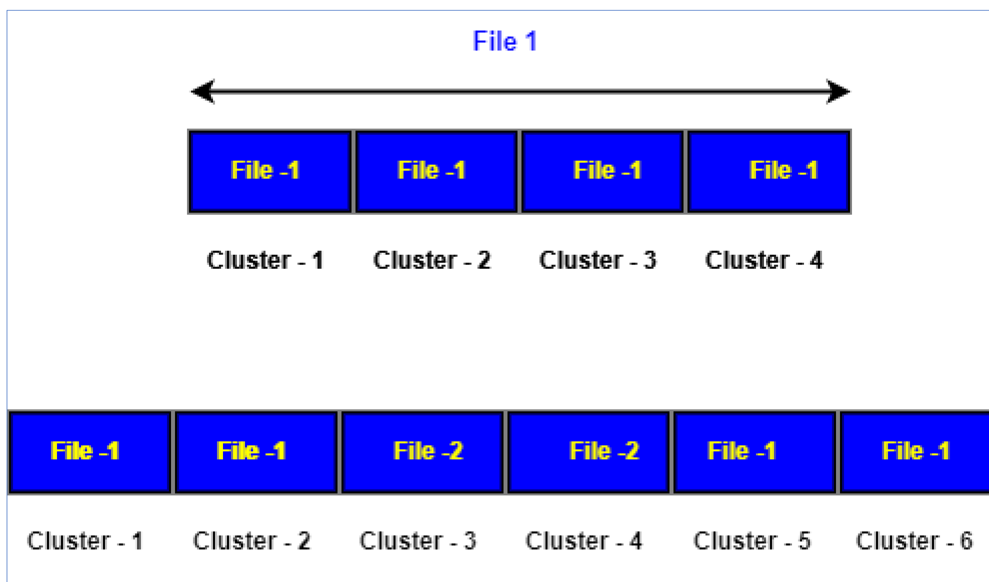
RAM Slack

Windows 95 ရှေ့ပိုင်းမှာတော့ လွတ်နေတဲ့ Sector နေရာကို RAM ပေါ်မှာရှိတဲ့ Data တွေကို random ယူပြီးထည့်ပါတယ်။ နောက်ပိုင်း Window Version တွေမှာတော့ လွတ်နေတဲ့ Sector နေရာကို 0x00 တွေထည့်လိုက်ပါတယ်။ ဥပမာ Sector Size 512 KB ရှိတယ်။ Sector ထဲမှာ သိမ်းဆည်းထားတဲ့ Data က 500 KB ရှိတယ်ဆိုရင် ကျန်လွတ်နေတဲ့ Space 12 KB မှာ **0x00** တွေထည့်လိုက်တာဖြစ်ပါတယ်။ Just For knowledge ပါ။ နောက်ပိုင်း Window Version တွေကြောင့် Ram Slack က သိပ်အသုံး မဝင်တော့ပါ။



Data Fragmentation

File တွေကို Read Write ပြုလုပ်တဲ့အခါမှာ Storage ပေါ်မှာ သိမ်းဆည်းထားတဲ့ Data တွေက Sector, Cluster ပေါ်မှာ တစ်ဆက်တည်းဖြစ်နေရင် Read/Write Speed ပိုမြန်ပါတယ်။ File Data တွေက ပြန့်ကျဲနေရင် Hard Disk ကို Fragmentation ပြုလုပ် ဖို့လိုအပ်မှာဖြစ်ပါတယ်။ ပုံမှာဆိုရင် File 1 က Cluster 1,2,5,6 ပေါ်မှာရှိနေပြီး File 2 က Cluster 3,4 နေရာမှာရှိနေပါတယ်။ တစ်ကယ်လို့ File 1 ကို Recover ယူမယ်ဆိုရင် File 2 ရဲ့ Data တွေပါ ပါလာနိုင်ပါတယ်။ ဆိုလိုချင်တာက Sector Base Recovery ပြုလုပ်ရာမှာ File Data သိမ်းဆည်းတဲ့ Sector, Cluster တွေက တစ်ဆက်တည်းဖြစ်မနေရင် (Fragmentation ဖြစ်နေလျှင်) Recovery ပြုလုပ်ရာမှာ အခက်ခဲရှိ နိုင်ပါ တယ်။



Master File Table

NTFS File System မှာ အဓိကအကျဆုံးကတော့ Master File Table (MFT) ပဲဖြစ်ပါတယ်။ File Size, File Name, File Date & Time, File Permission စတဲ့ Information တွေအကုန်ပါဝင်ပါတယ်။ NTFS File System ထဲမှာရှိတဲ့ File မှန်သမျှက MFT ထဲမှာ Entry အနေနဲ့ပါဝင်ပါတယ်။ MFT ကလဲ Entry တစ်ခုအနေနဲ့ Mater File Table ထဲမှာပါဝင်ပါတယ်။ NTFS File System ထဲကို File တွေရောက်လာတဲ့အမျှ ရောက်လာတဲ့ File တိုင်းရဲ့ Entry ကို MFT Table မှာသွားမှတ်ပါတယ် ဒါကြောင့် MFT Table ရဲ့ File Size ကလဲ Entry များလာတာနဲ့အမျှတိုးလာပါတယ်။ NFTS File System ရဲ့ Volume တိုင်းမှာ MFT ရှိပါတယ်။ File တစ်ခုကို ဖျက်လိုက်မယ်ဆိုရင် အဲဒီ File ရဲ့ MFT Entry ကို Free အနေနဲ့သတ်မှတ်လိုက်ပြီး နောက်တစ်ကြိမ် Entry တစ်ခုမှတ်မယ်ဆိုရင် သုံးလို့ရအောင်ထားလိုက်ပါတယ်။ ဖျက်လိုက်တဲ့ File ရဲ့ Disk Space နေရာမှာ အခြား File

တစ်ခုကဝင်ပြီးနေရာယူသွားရင်တောင် Entry နေရာမှာ လွတ်မသွားတဲ့အတွက် MFT Size က လျော့မသွားပါဘူး။ NFTS File System မှာ MFT Size တိုးလာရင် အသင့်ဖြစ်အောင် Space သီးသန့်ချန်ထားပါတယ်။ အဲဒီ Space ကို MFT Zone လို့ခေါ်ပါတယ်။

File View Mode Help

Evidence Tree

D:\
New Volume [NTFS]
[orphan]
[root]
#PDATE.7z
$BadClus
$Extend
$RECYCLE.BIN
$Secure
$UpCase
3uTools
AmpedAuthenticate
AmpedAuthenticate
AnyMP4 Temp

File List

Name	Size	Type	Date Modified
$BadClus	0	Regular File	7/21/2022 8:56:43 AM
$Bitmap	7,461	Regular File	7/21/2022 8:56:43 AM
$Boot	8	Regular File	7/21/2022 8:56:43 AM
$I30	24	NTFS Index All...	5/9/2023 1:50:19 AM
$LogFile	65,536	Regular File	7/21/2022 8:56:43 AM
$MFT	8,192	Regular File	7/21/2022 8:56:43 AM
$MFTMirr	4	Regular File	7/21/2022 8:56:43 AM
$Secure	1	Regular File	7/21/2022 8:56:43 AM
$TXF_DATA	1	NTFS Logged ...	5/9/2023 1:50:19 AM
$UpCase	128	Regular File	7/21/2022 8:56:43 AM
$Volume	0	Regular File	7/21/2022 8:56:43 AM

Thank You ...... !!!!

Aung Zaw Myo